Chapter 5
Safeguarding Classified Information

Section 1. General Safeguarding Requirements

5-100. General. Classified and unclassified sensitive SAP material must be stored in SAP CSA approved facilities only. Any deviations must have prior approval of the SAP CSA or designee.

Section 2. Control and Accountability

5-200. **General.** ***Contractors shall develop and maintain a system that enables control of SAP classified information and unclassified Program sensitive information for which the contractor is responsible.***

5-24)1. **Accountability.** ***Accountability of classified SAP material shall be determined and approved in writing by the CSA or designee at the time the SAP is approved.*** A separate accountability control system may be required for each SAP.

5-202. Annual Inventory. An annual inventory of accountable SAP classified material may be required. The results of the inventory and any discrepancies may be required to be reported in writing to the PSO.

5-203. Collateral classified material required to support a SAP contract may be transferred within SAP controls. ***Transfer will be accomplished in a manner that will not compromise the SAP or any classified information. The PSO will provide oversight for collateral classified material maintained in the SAP.*** Collateral classified material generated during the performance of a SAP contract may be transferred from the SAP to the contractor's collateral classified system. The precautions required to prevent compromise will be approved by the PSO.

Section 3. Storage and Storage Equipment

(not further supplemented)

Section 4. Transmission

5-400. General. *SAP classified material shall be transmitted outside the contractor's facility in a manner that prevents loss or unauthorized access.*

5-401. **Preparation.** *AU classified SAP material will be prepared, reproduced, and packaged by Program-briefed personnel in approved Program facilities.*

5-402. **Couriers.** *The PSO through the CPSO will provide detailed courier instructions to couriers when hand-carrying SAP material The CPSO will provide the courier with an authorization letter.* Report any travel anomalies to the CPSO as soon as practical. The CPSO will notify the PSO.

5-403. **Secure Facsimile and/or Electronic Transmission.** Secure facsimile and/or electronic transmission encrypted communications equipment may be used for the transmission of Program classified information. *When secure facsimile and/or electronic transmission is permitted, the PSO or other Government cognizant security reviewing activity will approve the system in writing.* Transmission of classified Program material by this means may be receipted for by an automated system generated message that transmission and receipt has been accomplished. For TOP SECRET documents a receipt on the secure facsimile may be required by the PSO.

5-404. **U.S. Postal Mailing.** A U.S. Postal mailing channel, when approved by the PSO, may be established to ensure mail is received only by appropriately cleared and accessed personnel.

5-405. **TOP SECRET Transmission.** *TOP SECRET (TS) SAP will be transmitted via secure data transmission or via Defense Courier Service unless other means have been authorized by the PSO.*

Section 5. Disclosure

5-500. **Release of Information.** ***Public release of SAP information is not authorized without written authority from the Government as provided for in U.S. Code, Titles 10 and 42.*** Any attempt by unauthorized personnel to obtain Program information and sensitive data will be reported immediately to the Government Program Manager (GPM) through the PSO using approved secure communication channels.

Section 6. Reproduction

5-600. **General.** ***Program material will be reproduced on equipment specifically designated by the CPSO*** and may require approval by the PSO. The CPMS and CPSOs may be required to prepare written reproduction procedures.

5-601. The PSO or designee may approve reproduction of TS material.

Section 7. Disposition and Retention

5-700. Deposition. CPSOS may be required to inventory, dispose of, request retention, or return for disposition all classified SAP-related material (including AIS media) at contract completion and/or close-out. ***Request for proposal (RFP), solicitation, or bid and proposal collateral classified and unclassified material contained in Program files will be reviewed and screened to determine appropriate disposition (i.e., destruction, request for retention). Disposition recommendations by categories of information or by document control number, when required, will be submitted to the PSO for concurrence. Requests for retention of classified information (SAP and non-SAP) will be submitted to the Contracting Officer, through the PSO for review and approval. Requirements for storage and control of materials approved for retention will be approved by the PSO.***

5-701. Retention of SAP Material. The contractor may be required to submit a request to the Contracting Officer (CO), via the PSO, for authority to retain classified material beyond the end of the contract performance period. The request will also include any retention of Program-related material. ***The contractor will not retain any Program information unless specifically authorized in writing by the Contracting Officer. Storage and control requirements of SAP materials will be approved by the PSO.***

5-702. **Destruction.** ***Appropriately indoctrinated personnel shall ensure the destruction of classified SAP data.*** The CSA or designee may determine that two persons are required for destruction. Nonaccountable waste and unclassified SAP material may be destroyed by a single Program-briefed employee.

Section 8. Construction Requirements

5-800. General. Establishing a Special Access Program Facility (SAPF). Prior to commencing work on a SAP, the contractor may be required to establish an approved SAPF to afford protection for Program classified information and material. ***Memorandums of Agreement (MOA) are required prwr to allowing SAPS with different CSAS to share a SAPF.***

5-801. **Special Access Program Facility.**

a. A SAPF is a program area, room, group of rooms, building, or an enclosed facility accredited by the PSO where classified SAP Program business is conducted. ***SAPFs will be afforded personnel access control to preclude entry by unauthorized personnel. Non-accessed persons entering a SAPF will be escorted by an indoctrinated person.***

b. A Sensitive Compartmented Information Facility (SCIF) is an area, room, building, or installation that is accredited to store, use, discuss, or electronically process SCI. The standard and procedures for a SCIF are stated in DCIDs 1/19 and 1/21.

c. ***SAPFS accredited prior to implementation of this Supplement will retain accreditation until no longer required or recertification is required due to major modification of the external perimeter, or changes to the Intrusion Detection System (IDS), which affects the physical safeguarding capability of the facility.***

d. ***Physical security standards will be stated in the Government's RFP, RFQ, contract, or other precontract or contractual document.***

e. The need-to-know (NTK) of the SAP effort may warrant establishment of multi-compartments within the same SAPF.

f. *There may be other extraordinary or unique circumstances where existing physical security standards are inconsistent with facility operating requirements, for example, but not limited to, research and test facilities or production lines. ***Physical security requirements under these circumstances will be established on a case-by-case basis and approved by the PSO/Contracting Officer, as appropriate. (Note: as approved by the CSA at establishment of the SAP.)***

g. The PSO will determine the appropriate security countermeasures for discussion areas.

5-802. **Physical Security Criteria Standards.**

a. DCID 1/21 standards may apply to a SAPF when one or more of the following criteria are applicable:

(1) State-of-the-art technology as determined by CSAS to warrant enhanced protection.

(2) Contractor facility is known to be working on specific critical technology.

(3) Contractor facility is one of a few (3 or less) known facilities to have the capability to work on specific critical technology.

(4) TOP SECRET or SECRET material is maintained in open storage.

(5) A SAPF is located within a commercial building, and the contractor does not control all adjacent spaces.

(6) SCI or Intelligence Sources and methods are involved.

(7) Contractors or technologies known to be a target of foreign intelligence services (FIS).

b. The NISPOM baseline closed area construction requirements with Sound Transmission Class (STC) in accordance with DCID 1/21, Annex E and intrusion alarms in accordance with Annex B, DCID 1/21 may apply to a SAPF when one of the following criteria are applicable.

(1) Not state-of-the-art technology and the technology is known to exist outside U.S. Government control.

(2) The SAP is a large-scale weapon system production program.

(3) No open storage of Confidential SAP material in a secure working area unless permitted by the PSO on a case-by-case basis.

(4) A SAPF located within a controlled access area.

(5) Intelligence related activities.

c. The PSO may approve baseline closed area construction requirements as an additional option for some SAP program areas.

5-803. **SAP Secure Working Area.** The PSO may approve any facility as a SAP Secure Working Area. Visual and sound protection may be provided by a mix of physical construction, perimeter control, guards, and/or indoctrinated workers.

5-804. Temporary **SAPF.** The PSO may accredit a temporary SAPF.

5-S05. **Guard** Response.

a. ***Response to alarms will be*** in ***accordance with DCID 1/21, or***

b. ***The NISPOM***

c. ***Response personnel will remain at the scene until released by the CPSO or designated representative.***

NOTE: The CPSO will immediately provide notification to the PSO if there is evidence of forced entry, with a written report to follow within 72 hours.

5-806. **Facility Accreditation.**

a. Once a facility has been accredited to a stated level by a Government Agency, that accreditation should be accepted by any subsequent agency.

b. For purposes of co-utilization, costs associated with any security enhancements in a SCIF or SAPF above preexisting measures may be negotiated for reimbursement by the contractor's contracting officer or designated representative. Agreements will be negotiated between affected organizations.

c. ***If a previously accredited SAPF becomes inactive for a-period not to exceed one year, the SAP accreditation will be reinstated by the gaining accrediting agency provided the following is true:***

(1) The threat in the environment surrounding the SAPF has not changed;

(2) No modifications have been made to the SAPF which affect the level of safeguarding;

(3) The level of safeguarding for the new Program is comparable to the previous Program;

(4) The SAPF has not lost its SAP accreditation integrity and the contractor has maintained continuous control of the facility.

(5) A technical surveillance countermeasure survey (TSCM) maybe required.

NOTE: Previously granted waivers are subject to negotiation.

5-807. **Prohibited Items.** Items that constitute a threat to the security integrity of the SAPF (e.g., cameras or recording devices) are prohibited unless authorized by the PSO. All categories of storage media entering and leaving the SAPFS may require the PSO or his/her designated representative approval.